

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341337

(43)Date of publication of application : 08.12.2000

(51)Int.Cl.

H04L 12/56

H04L 12/46

H04L 12/28

H04L 12/66

(21)Application number : 11-153248

(71)Applicant : NEC CORP

(22)Date of filing : 01.06.1999

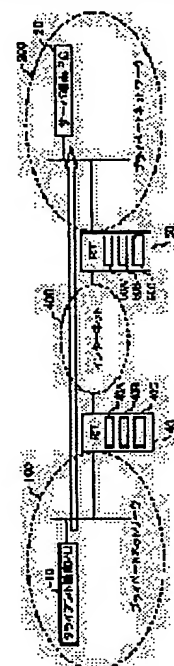
(72)Inventor : SATO TAKESHI

(54) INTER-PRIVATE-NETWORK CONNECTION SYSTEM AND ITS METHOD BY IP MASQUERADE

(57)Abstract:

PROBLEM TO BE SOLVED: To effectively utilize a global IP address.

SOLUTION: The inter-private-network connection system by an IP masquerade to connect private networks with an IP masquerade function via the Internet is provided with routers 40, 50 that are placed to each private network and have an OP masquerade function. The router 40(50) has a port number reservation table 40C(50C) that stores in common a plurality of reservation host names for the terminals requesting connection in advance and a plurality of internal recognition port numbers corresponding to the reservation host names respectively, each router references the port number reservation table and uses an internal reservation port number for a sender port number of a packet in the case of connection to the Internet, recognizes a reservation host name from the internal reservation port number used for the packet sender port number in the case of connection to the private network, and gives the packet to the terminal with the recognized reservation host name.



LEGAL STATUS

[Date of request for examination] 23.05.2000

[Date of sending the examiner's decision of rejection] 12.10.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-341337

(P2000-341337A)

(43)公開日 平成12年12月8日(2000.12.8)

(51)Int.Cl. ⁷	識別記号	F I	テ-マコード*(参考)
H 0 4 L	12/56	H 0 4 L 11/20	1 0 2 D 5 K 0 3 0
	12/46	11/00	3 1 0 C 5 K 0 3 3
	12/28	11/20	B 9 A 0 0 1
	12/68		

審査請求 有 請求項の数 9 O L (全 10 頁)

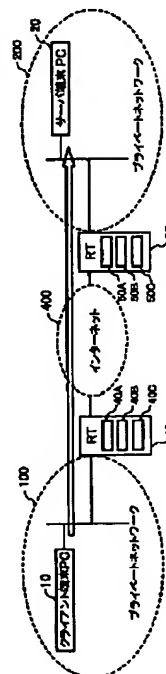
(21)出願番号	特願平11-153248	(71)出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22)出願日	平成11年6月1日(1999.6.1)	(72)発明者	佐藤 壮 東京都港区芝五丁目7番1号 日本電気株式会社内
		(74)代理人	100104400 弁理士 浅野 雄一郎
		Fターム(参考)	5K030 GA04 GA19 HB11 HB28 HC01 HD03 HD06 HD09 JT06 KA05 5K033 AA04 CB08 CC01 DA06 DB12 DB19 EC03 9A001 BB04 CC08 EE02 JJ25 KK31 LL03

(54)【発明の名称】 IPマスカレードによるプライベートネットワーク間接続システム及び方法

(57)【要約】

【課題】 グローバルIPアドレスの有効活用を可能にする。

【解決手段】 インターネットを介してプライベートネットワーク間をIPマスカレード機能で接続するためのIPマスカレードによるプライベートネットワーク間接続システムに、プライベートネットワークの各々に設けられ、IPマスカレード機能を有するルータ40,50を備え、ルータは、予め接続が要求される端末の複数の予約ホスト名、予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータで共通に保持するポート番号予約テーブル40C,50Cを有し、ルータは、ポート番号予約テーブルを参照して、インターネットへの接続時に、パケットの送信元ポート番号として内部予約ポート番号を用い、プライベートネットワークへの接続時に、パケットの送信元ポート番号として用いられた内部予約ポート番号から予約ホスト名を認識して、認識された予約ホスト名の端末にパケットを渡す。



【特許請求の範囲】

【請求項1】 インターネットを介してプライベートネットワーク間をIPマスカレード機能で接続するためのIPマスカレードによるプライベートネットワーク間接続システムにおいて、

前記プライベートネットワークの各々に設けられ、IPマスカレード機能を有するルータを備え、前記ルータは、

予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータで共通に保持するポート番号予約テーブルを有し、

前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用い、

前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡すことを特徴とするIPマスカレードによるプライベートネットワーク間接続システム。

【請求項2】 前記ルータの各々は、DHCP機能を用いて前記端末がサーバ機能を有するものに予約ホスト名を割当て、さらに、DNS機能を用いてテーブル前記インターネットを介して対向する前記ルータに相互に予約ホスト名を問い合わせ、前記ポート番号予約テーブルが共通の予約ホスト名を保持することを可能にすることを特徴とする、請求項1に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項3】 前記ポート番号予約テーブルは、複数の前記内部予約ポート番号に対応して仮IPアドレスを各ルータで個別に保持し、パケットの送信先プライベートIPアドレスとして前記仮IPアドレスが用いられるようにすることを特徴とする、請求項1に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項4】 前記インターネットへの接続時に、前記ポート番号予約テーブルを参照し、前記ルータは、パケットの送信元ポート番号の番号を、パケットの送信先プライベートIPアドレスとして用いた前記仮IPアドレスに対応する内部予約ポート番号に変換することを特徴とする、請求項3に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項5】 前記送信元ポート番号は、パケットの送信先プライベートIPアドレスとして用いた前記仮IPアドレスに対応して前記ポート番号予約テーブルに保持されることを特徴とする、請求項4に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項6】 前記ポート番号予約テーブルはパケットの送信先プライベートIPアドレスとして用いた前記仮IPアドレスに対応して送信先グローバルIPアドレスを保持することを特徴とする、請求項3に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項7】 前記ポート番号予約テーブルに保持されている内容が一定期間使用されていない場合にはその内容を削除することを特徴とする、請求項1に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項8】 前記プライベートネットワーク間の接続は、広域ネットワーク、インターネットを介して行われることを特徴とする、請求項1に記載のIPマスカレードによるプライベートネットワーク間接続システム。

【請求項9】 インターネットを介してプライベートネットワーク間をIPマスカレード機能で接続するためのIPマスカレードによるプライベートネットワーク間接続方法において、

前記プライベートネットワークの各々にルータを設けて、前記ルータにIPマスカレード機能をサポートさせる工程と、

予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータのポート番号予約テーブルで共通に保持する工程と、

前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用いる工程と、

前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡す工程を備えることを特徴とするIPマスカレードによるプライベートネットワーク間接続方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はIPマスカレードによるプライベートネットワーク間接続システム及び方法に関する。特に、本発明は、グローバルIPアドレス入手の削減、WAN回線契約チャンネル数の削減が図れるIPマスカレードによるプライベートネットワーク間接続システム及び方法に関する。

【0002】

【従来の技術】図5は従来のIPマスカレードによるプライベートネットワーク間接続システムを説明する図である。なお、全図を通して同一の構成要素には同一の符号、記号を用いる。本図に示すように、プライベートネ

ットワーク100、200は、WAN (Wide Area Network; 広域ネットワーク) 回線300に接続され、さらにWAN回線300を介してインターネット400に接続されている。WAN回線300には、例えば、ISDN (Integrated Service Digital Network; 総合デジタルサービス網)、ATM (Asynchronous Transfer Mode; 非同期転送モード) が適用されていてもよい。

【0003】プライベートネットワーク100にはクライアント端末PC1 (Personal Computer)、インターネット400にはサーバ端末PC3が接続され、プライベートネットワーク200にはサーバ端末PC2が接続されているとする。インターネット400にはインターネットサービスプロバイダーが所有するゲートウェイISP6、7が設けられ、ゲートウェイISP6、7はWAN400とインターネット400との間の緩衝を果たす。

【0004】プライベートネットワーク100、200にはルータ4、5が設けられ、パケットの行き先案内を行う。なお、パケットはIPアドレスとデータとからなり、IPアドレスはデータの送信元IPアドレスとデータの送信先IPアドレスとからなる。ルータ4はIP (Internet Protocol) マスカレード (Masquerade) 機能をサポートする。マスカレード機能はプライベートネットワーク100内にプライベートIPアドレスを有するクライアント端末PC1の複数が同時にインターネット400に同時に接続要求を行うと、パケットの複数送信元のプライベートIPアドレスを1つのグローバルIPアドレスに変換し、個々の接続要求はポート番号で区別される。

【0005】このようにして、プライベートネットワーク100からインターネット400に要求するクライアント端末PC1の複数の同時接続が1つのグローバルIPアドレスで可能になる。他方、ルータ5はNAT (Network Address Translation) 機能をサポートする。NAT機能はプライベートIPアドレスとグローバルIPアドレスとを1対1で相互に変換する機能である。プライベートネットワーク200内にプライベートIPアドレスを有するサーバ端末2が複数存在する場合、サーバ端末2の複数へのパケットでは複数宛先のグローバルIPアドレスの各々がプライベートIPアドレスに変換される。このようにして、インターネット400からプライベートネットワーク200に要求されるサーバ端末PC2の複数の同時接続が可能になる。

【0006】

【発明が解決しようとする課題】しかしながら、従来の上記IPマスカレードによるプライベートネットワーク間接続システムのプライベートネットワーク200で

は、グローバルIPアドレスを必要とするサーバ端末PC2の数だけインターネットプロバイダーからグローバルIPアドレスを入手する必要があるという第1の問題が発生する。すなわち、グローバルIPアドレスの有効活用を図る必要がある。

【0007】サーバ端末2がインターネット400を経由せず、直接にWAN回線300を経由するイントラネット接続によれば、グローバルIPアドレスの入手の問題は解決する。しかし、プライベートネットワーク100からWAN回線300を経由してインターネット400へのチャンネルと、プライベートネットワーク100からWAN回線300を経由してクライアントネットワーク200へのチャンネル、計2チャンネルのWAN回線を契約する必要があるという第2の問題が発生する。

【0008】したがって、本発明は上記問題点に鑑みて、グローバルIPアドレスを1つ入手するだけで、インターネットとイントラネットの同時接続を可能にし、WAN回線を1チャンネルに削減することを可能にするIPマスカレードによるプライベートネットワーク間接続システム及び方法を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明は前記問題点を解決するために、インターネットを介してプライベートネットワーク間をIPマスカレード機能で接続するためのIPマスカレードによるプライベートネットワーク間接続システムにおいて、前記プライベートネットワークの各々に設けられ、IPマスカレード機能を有するルータを備え、前記ルータは、予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータで共通に保持するポート番号予約テーブルを有し、前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用い、前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡すことを特徴とするIPマスカレードによるプライベートネットワーク間接続システムを提供する。

【0010】この手段により、IPマスカレード機能によりプライベートネットワークからインターネットへの同時接続時には1つのグローバルIPアドレスがあればよく、ポート番号予約テーブルを参照することによりインターネットからプライベートネットワークへの同時接続時にも1つのグローバルIPアドレスがあればよいので、グローバルIPアドレスの有効活用が可能である。好ましくは、前記ルータの各々は、DHCP機能を用いて前記端末がサーバ機能を有するものに予約ホスト名を

割当て、さらに、DNS機能を用いてテーブル前記インターネットを介して対向する前記ルータに相互に予約ホスト名を問い合わせ、前記ポート番号予約テーブルが共通の予約ホスト名を保持することを可能にする。

【0011】この手段により、前記ルータの各々のポート番号予約テーブルではDHCP機能、DNS機能を用いてサーバとしてサービスを提供する端末の名を予約ホスト名が共通に容易に保持されることが可能になる。好ましくは、前記ポート番号予約テーブルは、複数の前記内部予約ポート番号に対応して仮IPアドレスを各ルータで個別に保持し、パケットの送信先プライベートIPアドレスとして前記仮IPアドレスが用いられるようにし、さらに、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照し、前記ルータは、パケットの送信元ポート番号の番号を、パケットの送信先プライベートIPアドレスとして用いた前記仮IPアドレスに対応する内部予約ポート番号に変換する。

【0012】この手段により、インターネット接続時にパケットの送信元ポート番号の番号が内部予約ポート番号に変換されることにより、プライベートネットワーク接続時に変換された内部予約ポート番号が予約ホスト名に認識される。好ましくは、前記送信元ポート番号は、パケットの送信先プライベートIPアドレスとして用いた前記仮IPアドレスに対応して前記ポート番号予約テーブルに保持される。この手段により、プライベートネットワークへの逆の接続時に、仮IPアドレスに対応してパケットの送信先ポート番号は送信先プライベートIPアドレスに変換される。

【0013】好ましくは、前記ポート番号予約テーブルはパケットの送信先プライベートIPアドレスとして用いた前記仮IPアドレスに対応して送信先グローバルIPアドレスを保持する。この手段により、保持される送信先グローバルIPアドレスは送信すべき端末のプライベートネットワークについて1つである。すなわち、1つの送信先グローバルIPアドレスでプライベートネットワークに接続可能であるので、グローバルIPアドレスの活用が可能になる。好ましくは、前記ポート番号予約テーブルに保持されている内容が一定期間使用されていない場合にはその内容を削除する。

【0014】この手段により、使用されていない予約ホスト名に関連する内容の堆積がなくなり、処理煩雑を回避できる。好ましくは、前記プライベートネットワーク間の接続は、広域ネットワーク、インターネットを介して行われる。この手段により、インターネット、イントラネットを同時に接続しても、広域ネットワークの契約は1回線でよい。

【0015】さらに、本発明は、インターネットを介してプライベートネットワーク間をIPマスカレード機能で接続するためのIPマスカレードによるプライベートネットワーク間接続方法において、前記プライベートネ

ットワークの各々にルータを設けて、前記ルータにIPマスカレード機能をサポートさせる工程と、予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータのポート番号予約テーブルで共通に保持する工程と、前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用いる工程と、前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡す工程を備えることを特徴とするIPマスカレードによるプライベートネットワーク間接続方法を提供する。

【0016】この手段により、上記本発明と同様に、IPマスカレード機能によりプライベートネットワークからインターネットへの同時接続時には1つのグローバルIPアドレスがあればよく、ポート番号予約テーブルを参照することによりインターネットからプライベートネットワークへの同時接続時にも1つのグローバルIPアドレスがあればよいので、グローバルIPアドレスの有効活用が可能である。

【0017】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図1は本発明に係るIPマスカレードによるネットワーク構成を示す図である。本図では、説明の簡単化のために、図5におけるWAN回線300を省略してある。本図に示すプライベートネットワーク100、200の各々に設けられるルータ40、50はDHCP(Dynamic Host Configuration Protocol; 動的ホスト構成プロトコル)機能、DNS(Domain Name System)機能、IPマスカレード機能をサポートする。

【0018】これらの機能のサポートに伴って、ルータ40、50には、DHCPエントリテーブル40A、50A、DNSエントリテーブル40B、50B、ポート番号予約テーブル40C、50Cがそれぞれ実装される。プライベートネットワーク100のクライアント端末PC10の複数の数が同時にインターネット400に接続要求してそのうちの全部又はいくつかがインターネット400を経由してプライベートネットワーク200に、以下のように、イントラネット接続を行う。

【0019】図2はルータ40、50のDHCP機能を説明する図である。本図に示すように、クライアント端末PC10、サーバ端末PC20、サーバ端末PC21は、電源の投入後、DHCPクライアント機能を使用して該当するDHCPサーバのルータ40、50に対してプライベートIPアドレスを要求する(本図の①、②、

③参照)。クライアントID (本図の場合、端末のホスト名) と割当プライベートIPアドレスの対応付けによりルータ40、50は該当するクライアント端末PC10、サーバ端末PC20、サーバ端末PC21に対しプライベートIPアドレス: aaaa、dddd、eee eをそれぞれ割当てる。

【0020】

【表1】

RT40のDHCPエントリーテーブル40A

ホスト名	プライベートIPアドレス	予約ホスト名
PC10	a.a.a.a	—

【表2】

RT50のDHCPエントリーテーブル50A

ホスト名	プライベートIPアドレス	予約ホスト名
PC20	d.d.d.d	サーバ01
PC21	e.e.e.e	サーバ02

【0021】上記の表1、2に示すように、ルータ40、50のDHCPアドレスプール (割当てられるIPアドレスの束) には、ホスト名と割当IPアドレスの対応エントリーが存在しこの他に「予約ホスト名」のエントリーが設定される。この予約ホスト名は該当する端末 (ホスト名) が何らかの機能を提供するサーバを予めエントリーしておくもので、表2に示す予約ホスト名「サーバ01」は、例えば、テルネット (Telnet) サーバである。なお、テルネットは接続される相手のコンピュータを対話形式によって遠隔操作できるサービスである。

【0022】また、表1の予約ホスト名は本発明の機能を使用する全てのルータで統一がとれている必要があり、ルータ40、50が収容している全てのクライアント端末PC10、サーバ端末PC20、サーバ端末PC21のホスト名と重複しないように割当てられる。なお、クライアント端末PC10、サーバ端末PC20、サーバ端末PC21は、ホスト名PC10、ホスト名PC20、ホスト名PC30とそれぞれ名づけられる。また、ホスト名PC20、PC21に対して、表2に示すように、予約ホスト名はサーバ01、サーバ02のように名づけられる。

【0023】具体的には、本図の①に示すように、クライアント端末PC10からルータ40に対してDHCPを探すためのパケット (DHCP DISCOVER) が送信されると、ルータ40はクライアント端末PC10に回答パケット (DHCP OFFER) を送信してクライアント端末PC10のアドレス: aaaaを割当てる。同様に、本図の②に示すように、サーバ端末PC20からルータ50に対してDHCPを探すためのパケッ

ト (DHCP DISCOVER) が送信されると、ルータ50はサーバ端末PC20に回答パケット (DHCP OFFER) を送信してサーバ端末PC20のアドレス: ddddを割当てる。

【0024】同様に、本図の③において、サーバ端末PC21からルータ50に対してDHCPを探すためのパケット (DHCP DISCOVER) が送信されると、ルータ50はサーバ端末PC21に回答パケット (DHCP OFFER) を送信してサーバ端末PC21のアドレス: eeeeを割当てる。図3はルータ40、50のDNS機能を説明する図である。本図に示すサーバ端末PC20がテルネット (Telnet) サーバ機能を有し、クライアント端末PC10がテルネットクライアント機能を有しているとする。

【0025】また、クライアント端末PC10のDNSサーバ指定にルータ40が設定されていたとし、さらに、ルータ40のDNSサーバ検索エントリーにルータ50が指定されていたとする。また、ルータ40、50において、DHCPのアドレスプールはDNSエントリーテーブルに自動更新するようにしておく。これにより、ルータ40、50のDNSエントリーテーブルは下記の表3、5のようになる。

【0026】

【表3】

RT40のDNSエントリーテーブル40B

(DNS応答受信前)

ドメイン名	プライベートIPアドレス	予約ホスト名
PC10	a.a.a.a	—

【表4】

RT40のDNSエントリーテーブル40B

(DNS応答受信後)

ホスト名	プライベートIPアドレス	予約ホスト名
PC10	a.a.a.a	—
PC20	c.c.c.c	サーバ01

【表5】

RT50のDNSエントリーテーブル50B

ホスト名	プライベートIPアドレス	予約ホスト名
PC20	d.d.d.d	サーバ01
PC21	e.e.e.e	サーバ02

【0027】DHCPのアドレスプールと同じく、ルータ40、50はDNSエントリーテーブルには、ドメイン名 (説明を簡単にするために、ここではドメイン名 (FQDN; Fully Qualified Domain Name) にホスト名を使用している) とIP

アドレスとが存在しこの他に「予約ホスト名」のエントリーが設定される。例えば、本図の①に示すように、クライアント端末PC10は、サーバ端末PC20に対しドメイン（ホスト）名によりテルネット接続を行う場合、ルータ40に対しDNSの問い合わせを行う。

【0028】本図の②に示すように、ルータ40は、DNSエントリーテーブルの表3にサーバ端末PC20のエントリーが存在しない場合、DNSサーバ検索エントリーに従ってルータ50に対しDNSの問い合わせを行う。本図の③に示すように、ルータ50は、ドメイン名「PC20」のDNSの問い合わせを受信するとDNSエントリーテーブルの表4に「PC20」のエントリーが存在するため、ルータ40に対してDNSの返答を行う。DNSの応答においては、ドメイン名「PC20」とグローバルIPアドレスc.c.c.cの組み合わせではなく、予約ホスト名「サーバ01」とグローバルIPアドレスc.c.c.cの組み合わせで返答する。

【0029】本図の④に示すように、ルータ40はDNSの返答を受信すると、DNSメッセージヘッダのIdentification（識別）フィールドを確認す

ることにより、「PC20」で問い合わせたものに対し、「サーバ01」で返答を受信したことを認識する。この時点で、ルータ40は、表4のように、「PC20」に対し、予約ホスト名「サーバ01」のDNSエントリーを追加する。次に、ルータ40はクライアント端末PC10に対してDNSの返答を行う。ドメイン名は「PC20」にして、IPアドレスはルータ40が収容しているプライベートネットワーク内で使用していないサブネットの中から任意のプライベートIPアドレス「x.x.x.1」を入れてクライアント端末PC10に返す。

【0030】なお、ルータ40からクライアント端末PC10へのDNS応答は、DNSのキャッシュ時間を「0」に設定する必要がある。これは、クライアント端末PC10にある一定時間のキャッシュ時間を与えると、この期間内はDNSを使用せずにセッションを張り続けることになり、ポート番号予約テーブルのエントリーが作成できないためである。

【0031】

【表6】

RT40のポート番号予約テーブル40C

予約 ホスト名	プライベート ポート番号	内部予約 ポート番号	仮 IP アドレス	グローバル IP アドレス
サーバ01	—	2001	x.x.x.1	c.c.c.c
	—	2002	x.x.x.2	—
	—	2003	x.x.x.3	—
	—	2004	x.x.x.4	—
サーバ02	—	2005	x.x.x.5	—
	—	2006	x.x.x.6	—
	—	2007	x.x.x.7	—
	—	2008	x.x.x.8	—

【表7】

RT50のポート番号予約テーブル50C

予約 ホスト名	プライベート ポート番号	内部予約 ポート番号	仮 IP アドレス	グローバル IP アドレス
サーバ01	—	2001	y.y.y.1	—
	—	2002	y.y.y.2	—
	—	2003	y.y.y.3	—
	—	2004	y.y.y.4	—
サーバ02	—	2005	y.y.y.5	—
	—	2006	y.y.y.6	—
	—	2007	y.y.y.7	—
	—	2008	y.y.y.8	—

【表8】

RT40のポート番号予約テーブル40C

(テルネット(SYN)受信後)

予約 ホスト名	プライベート ポート番号	内部予約 ポート番号	仮 IP アドレス	グローバル IP アドレス
サーバ01	1024	2001	x. x. x. 1	c. c. c. c
	—	2002	x. x. x. 2	—
	—	2003	x. x. x. 3	—
	—	2004	x. x. x. 4	—
サーバ02	—	2005	x. x. x. 5	—
	—	2006	x. x. x. 6	—
	—	2007	x. x. x. 7	—
	—	2008	x. x. x. 8	—

【0032】上記の表6、7のポート番号予約テーブルについては、全ルータ40、50に実装する必要がある。表6、7は予約ホスト名、プライベートポート番号、内部予約ポート番号、仮IPアドレス、グローバルIPアドレスで構成されている。上記の予約ホスト名は、前述のように、予め取り決めておくサーバのホスト名であり、全てのルータ40、50で統一が取れている必要がある。上記のプライベートポート番号はルータ40、50のプライベートネットワーク100、200内のクライアント端末PC10、サーバ端末PC20、サーバ端末PC21が任意のパケットを送信する際の送信元ポート番号が入る(後述参照)。

【0033】上記の内部予約ポート番号は予め取り決めておく送信元のポート番号であり、全てのルータ40、50で統一がとれている必要がある。例えば、表6、7、8に示す内部予約ポート番号「2001」、「2002」、「2003」、「2004」は予約ホスト名「サーバ01」を特定し、内部予約ポート番号「2005」、「2006」、「2007」、「2008」は予約ホスト名「サーバ02」を特定する。上記の仮IPアドレスは、送信先の任意のプライベートIPアドレスを割り与える。内部予約ポート番号と、仮IPアドレスの対応付けは、後述するように、管理される。上記DNSの問い合わせによるプライベートIPアドレスは一時的に割り与えるもので仮IPアドレスとして使用される。この場合、ルータ40はポート番号予約テーブルの表6を更新する。

【0034】ルータ40では、表6、8に示すように、内部予約ポート番号「2001」、「2002」、「2003」、「2004」、「2005」、「2006」、「2007」、「2008」に対して、仮IPアドレス「x. x. x. 1」、「x. x. x. 2」、「x. x. x. 3」、「x. x. x. 4」、「x. x. x. 5」、「x. x. x. 6」、「x. x. x. 7」、

「x. x. x. 8」がそれぞれ対応つけられて管理される。ルータ50では、表7に示すように、内部予約ポート番号「2001」、「2002」、「2003」、「2004」、「2005」、「2006」、「2007」、「2008」に対して、仮IPアドレス「y. y. y. 1」、「y. y. y. 2」、「y. y. y. 3」、「y. y. y. 4」、「y. y. y. 5」、「y. y. y. 6」、「y. y. y. 7」、「y. y. y. 8」がそれぞれ対応つけて管理される。

【0035】上記グローバルIPアドレスでは、仮IPアドレスとして「x. x. x. 1」が設定されると、これに対応して、表6、8に示すように、ルータ40のIPマスカレードで使用される送信先グローバルIPアドレス「c. c. c. c」が設定される。

【0036】図4はIPマスカレード機能を使用しているルータ40、50のプライベートネットワーク間の転送を説明する図である。本図の①において、前述のように、ルータ40からDNSの返答を受信したクライアント端末PC10は、パケットの送信先IPアドレスを、ルータ40が管理する仮IPアドレス「x. x. x. 1」に設定し、送信元ポート番号を、1024以上に一例として1024に設定する。この場合、仮IPアドレスとして「x. x. x. 1」が設定されると、これに対応して、表8に示すように、プライベートポート番号1024が設定される。

【0037】パケットの送信先ポート番号を23にしてテルネットセッションが開始される。つまり、テルネット接続要求(Telnet(SYN))が行われる。この時点で、ルータ40は、表3(c)に示すようにプライベートポート番号と内部予約ポート番号の対応が更新される。この場合、送信先ポートは、前述のように、ポート番号23であり、これはwell-known port(よく知られたポート)である。パケットの送信先プライベートIPアドレスは仮IPアドレス「x.

x. x. 1」に設定され、送信元プライベートIPアドレスは「a. a. a. a」に設定される。

【0038】本図の②において、ルータ40は、ポート番号予約テーブルの表6に従って、送信先のプライベートIPアドレスを仮IPアドレス「x. x. x. 1」からグローバルIPアドレス「c. c. c. c」に変換し、且つ、送信元ポート番号をクライアント端末PC10が設定してきたポート番号「1024」から内部予約ポート番号「2001」に変更して、グローバルネットワーク側にパケットを送信する。また、送信元プライベートIPアドレスは「a. a. a. a」は送信元グローバルIPアドレス「b. b. b. b」に変更される。

【0039】本図の③において、グローバルネットワーク経由で本パケットを受信したルータ50は、送信元ポート番号を確認し、ポート番号予約テーブル表7から送信元ポート番号が「2001」であることからサーバ端末PC20宛てのパケットであることが分かったため、サーバ端末PC20に対してパケットを送信する。また、送信先グローバルIPアドレス「c. c. c. c」が送信先プライベートIPアドレス「d. d. d. d」に変換される。サーバ端末PC20から端子PC10への返りのパケットは、端末PC10から端末PC20へのパケット送信と逆の変換を行うことにより可能になる（本図④、⑤、⑥参照）。上記例の続きとして、テルネットの接続要求に対する応答確認（Telnet（ACK/SYN））を行う。

【0040】但し、ルータ50は、本来ならばIPマスカレード機能によってプライベートネットワーク側のサーバ端末PC20からパケットを受信した場合、送信元ポート番号を変更するが、送信元ポート番号がよく知られたポート（well-known port（例えば、23番））である場合は、ポート番号を変更しないようにする。この一連の処理によって、予約ホスト名、プライベートポート番号、内部予約ポート番号、仮IPアドレス、グローバルIPアドレスの一連のエントリを完成させることができ、IPマスカレード機能を使用しているルータ40、50のプライベートネットワーク間で、パケットの転送が可能になる。なお、ポート番号予約テーブルのエントリ削除は、タイマによって行う。ある一定期間エントリを使用しなかった場合、該

当エントリは削除される。不使用エントリの堆積に起因する処理煩雑を避けるためである。

【0041】

【発明の効果】以上説明したように、本発明によれば、IPマスカレード機能によりプライベートネットワークからインターネットへの同時接続時には1つのグローバルIPアドレスがあればよく、ポート番号予約テーブルを参照することによりインターネットからプライベートネットワークへの同時接続時にも1つのグローバルIPアドレスがあればよいので、グローバルIPアドレスの有効活用が可能である。また、広域ネットワークを介してインターネット、イントラネットへの同時接続は、広域ネットワーク回線の1チャンネルのみの契約で可能になる。

【図面の簡単な説明】

【図1】図1は本発明に係るIPマスカレードによるネットワーク構成を示す図である。

【図2】図2はルータ40、50のDHCP機能を説明する図である。

【図3】図3はルータ40、50のDNS機能を説明する図である。

【図4】図4はIPマスカレード機能を使用しているルータ40、50のプライベートネットワーク間の転送を説明する図である。

【図5】図5は従来の従来のIPマスカレードによるプライベートネットワーク間接続システムを説明する図である。

【符号の説明】

10…クライアント端末PC

20、21…サーバ端末PC

40、50…ルータ

40A…ルータ40のDHCPエントリテーブル

40B…ルータ40のDNSエントリテーブル

40C…ルータ40のポート番号予約テーブル

50A…ルータ50のDHCPエントリテーブル

50B…ルータ50のDNSエントリテーブル

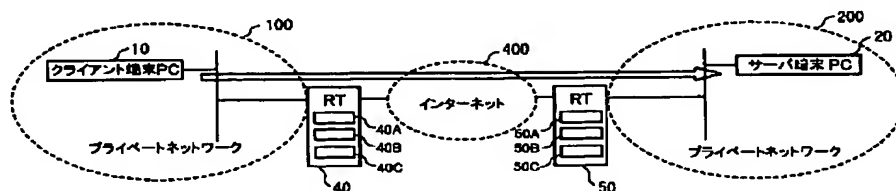
50C…ルータ50のポート番号予約テーブル

100、200…プライベートネットワーク

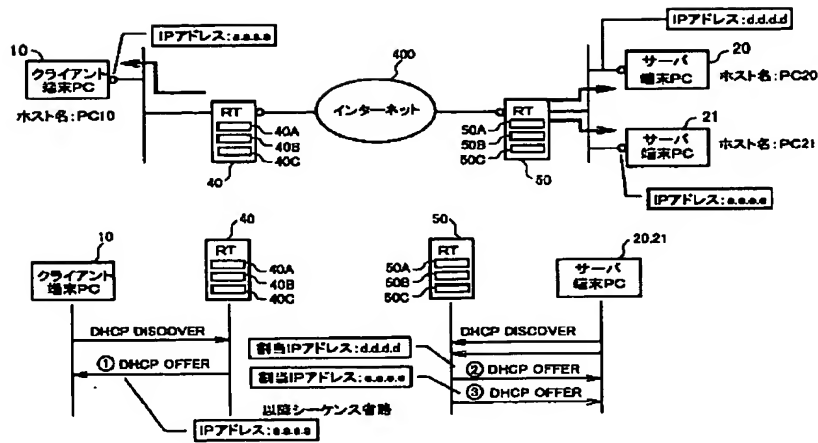
300…広域ネットワーク

400…インターネット

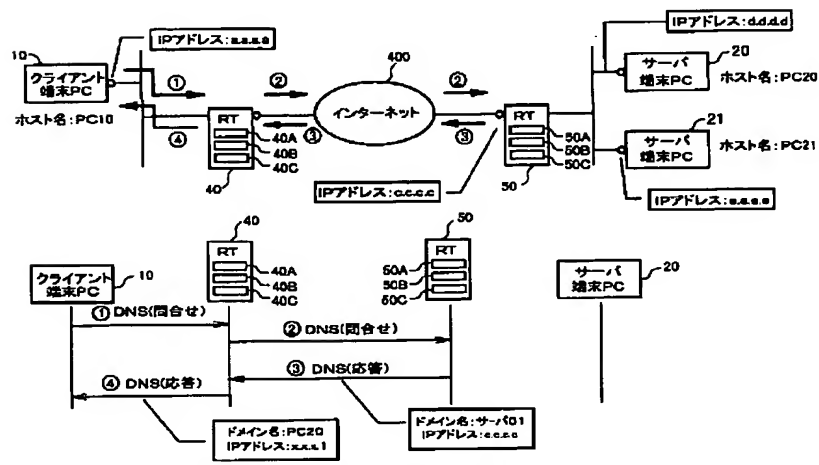
【図1】



【図2】

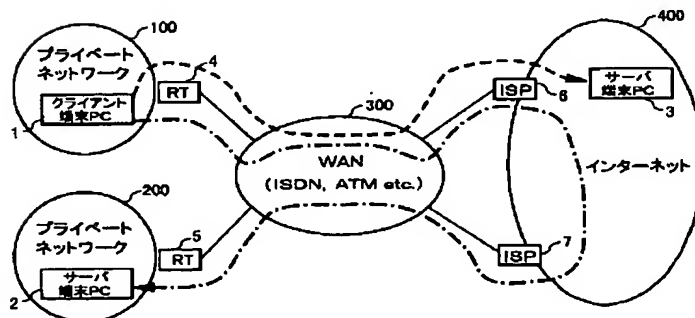


【図3】



・説明を簡単にするため、ドメイン名とホスト名を同じにしている

【図5】



【図4】

